EXHIBIT 15

SYMANTEC'S STATEMENT OF ANTICIPATED PROOFS

Symantec expects that it will offer the following proof at trial, subject to revision based upon the Court's rulings any pending motions, or in response to new matters introduced in SRI's Statement of Anticipated Proofs. In addition to the items identified below, Symantec intends to prove the matters identified in its Answer and Counterclaims to SRI's First Amended Complaint, interrogatory answers and in the expert reports of its expert witnesses. Symantec also intends to offer proof on the issues of fact and issues of law identified by the parties in this Joint Pretrial Order.

For the Court's convenience, the claims asserted against Symantec will be referred to herein as the "asserted claims." The particular claims asserted against Symantec are:

Claims asserted against Symantec	• '203 patent: claims 1-2, 4, 6, 12-13, 15, 17 • '615 patent: claims 1-2, 4, 13-14, 16

I. INVALIDITY OF THE PATENTS-IN-SUIT

Symantec will introduce proof that:

1. The asserted claims of the '203 and '615 patents are invalid under 35 U.S.C. § 102 as anticipated, based upon the following prior art publications and systems or products:

- P. Porras and A. Valdes, "Live Traffic Analysis of TCP/IP Gateways," ("*Live Traffic*" various versions);
- P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances," Proceedings of the 20th National Information Systems Security Conference, pp. 353-365, October 9, 1997 ("*Emerald 1997*");
- L. Todd Heberlein et al., "A Network Security Monitor," Proc. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, pp. 296-304, May 1990 ("*NSM 1990*");
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "Internetwork Security Monitor," Proc. of the 15th National Computer Security Conference, pp. 262-271, October 1992 ("*ISM 1992*");

- B. Mukherjee, L.T. Heberlein, K.N. Levitt, "Network Intrusion Detection," IEEE Network, Vol. 8 No. 3, pp. 26-41, June 1994 ("*NID 1994*");
- Steven R. Snapp et al., "Intrusion Detection Systems (IDS): A Survey of Existing Systems and a Proposed Distributed IDS Architecture," CSE-91-7, Feb. 1991 ("*DIDS Feb. 1991*");
- Steven R. Snapp et al., "DIDS (Distributed Intrusion Detection System) – Motivation, Architecture, and An Early Prototype," Proc. 14th National Computer Security Conference, pp. 167-173, October 1991 ("*DIDS Oct. 1991*");
- S. Staniford-Chen et al., "GrIDS – A Graph Based Intrusion Detection System for Large Networks," 19th National Information Systems Security Conference, pp. 361-370, October 1996 ("*GrIDS 1996*");
- Steven Cheung et al., "The Design of GRIDS: A Graph-Based Intrusion Detection System," Technical Report, UC Davis Department of Computer Science, Davis California, May 14, 1997 ("*GrIDS 1997*");
- "RealSecure Release 1.0 for Windows NT 4.0 A User's Guide and Reference Manual";
- "NetRanger User's Guide Version 1.3.1," WheelGroup Corporation, 1997 ("*NetRanger Manual*");
- Network Security Monitor ("NSM");
- Distributed Intrusion Detection System ("DIDS");
- Graph-based Intrusion Detection System ("GrIDS");
- NetRanger; and
- ISS RealSecure.

2. The asserted claims of the '203 and '615 patents are invalid under 35 U.S.C. § 103 as obvious based on a combination of two or more of the following references, or based upon an obvious modification to one or more of the following references:

- All prior art publications and systems or products listed in (1) above;
- L.T. Heberlein, B. Mukherjee, K.N. Levitt, "A Method to Detect Intrusive Activity in a Networked Environment," Proc. 14th National Computer Security Conference, pp. 362-371, Oct. 1991;
- Emerald 1997 in combination with additional references regarding the Network Security Monitor, the Distributed Intrusion Detection System, the Graph Based

Intrusion Detection System, the ISS RealSecure system, and the NetRanger system;

- SunScreen EFS Configuration and Management Guide, Release 1.1, Rev. A, Sun Microsystems, June 1997;
- CERT Advisory CA-1996-21 TCP Syn Flooding and IP Spoofing Attacks;
- CERT Advisory CA-1996-26 "Denial-of-Service Attack via Ping, Dec. 18, 1996.

3. The asserted claims of the '203 and '615 patents are invalid under 35 U.S.C. § 112 as invalid for failure to satisfy the written description requirement and failure to satisfy the best mode requirement.

4. Rebuts SRI's assertions of evidence of secondary indicia of nonobviousness, and any evidence of a purported nexus between alleged secondary indicia and the purported invention(s) of the '203 and '615 patents.

5. Objective evidence of obviousness that supports a finding that the asserted claims were obvious over the prior art.

II. UNENFORCEABILITY OF THE PATENTS-IN-SUIT

Symantec will introduce proof that:

6. Individuals associated with the filing or prosecution of the '203 and '615 patents either withheld information from the United States Patent & Trademark Office (the "PTO") or misrepresented information to the PTO.

7. The information withheld or misrepresented by individuals associated with the filing or prosecution of the '203 and '615 patents was material.

8. The information withheld or misrepresented by individuals associated with the filing or prosecution of the '203 and '615 patents was withheld or misrepresented with the intent to mislead or deceive the PTO.

III. NONINFRINGEMENT

Symantec's iForce IDS, ManHunt 3.0, Symantec Network Security 4.0, and Symantec Network Security 7100 Series appliances will be referred to as the "ManHunt Products."

Symantec's Incident Manager 3.0 and Security Information Manager 9500 Series appliances will be referred to as the "Manager Products."

Symantec's Gateway Security 5400, 5600 and 1600 Series appliances will be referred to as the "SGS Products."

Symantec will introduce proof that:

A. ManHunt Products

9. Rebuts SRI's assertion that Symantec directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by making, using, selling, or offering to sell the ManHunt Products.

10. Rebuts SRI's assertion that any Symantec customer directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by using the ManHunt Products.

11. Rebuts SRI's assertion that Symantec, with the requisite intent and knowledge, actively induced its customers to infringe the asserted claims of the '203 or '615 patents by use of the ManHunt products.[1]

B. SGS Products + Manager Products

12. Rebuts SRI's assertion that Symantec directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by making, using, selling, or offering to sell the SGS Products in combination with the Manager Products.

[1] Symantec understands that SRI is no longer asserting contributory infringement against any Symantec product.

13. Rebuts SRI's assertion that any Symantec customer directly infringes the '203 or '615 patents, either literally or under the doctrine of equivalents, by using the SGS Products in combination with the Manager Products in the manner that SRI alleges to be infringing.

14. Rebuts SRI's assertion that Symantec, with the requisite intent and knowledge, actively induced its customers to infringe the asserted claims of the '203 or '615 patents by using the SGS Products in combination with the Manager Products.